Cookie and Browser Storage Policy

Cookies and browser storage used by Lumez, their purposes and configured durations, and the controls available to users.

Version: 2026-09-18.1
Last updated: 2026-09-18

Responsible provider

64.117.651 ARTHUR GOMES DE FREITAS CARDOZO

CNPJ 64.117.651/0001-49

10A RUA DOUTOR MONTEIRO, 864, CASA, CENTRO, ARROIO GRANDE/RS, CEP 96330-000 - Brasil

Official domain: https://lumez.digital-directive.com

Privacy and support: arthurgfcardozo@gmail.com

Initial market: South America

Infrastructure: AWS, Google Cloud, Vercel and infrastructure operated by Digital Directive

Digital Directive is the trade name declared by the owner. Lumez is the product covered by these documents; other products are not automatically included.

1. Scope and status of this inventory

This policy describes cookies and browser storage identified in Lumez, a product offered by Digital Directive at lumez.digital-directive.com. Initial markets are in South America. Cookies are small records sent with relevant website requests; local storage keeps information in the browser and is not automatically sent with every request.

The inventory reflects application settings and the authentication library used by the reviewed version. It does not constitute an independent audit of every script or service deployed in production. A configured duration is not a guarantee that a browser will retain a record for that entire period.

2. Authentication and session cookies

The cookies below support sign-in and access to the requested account. They are set by the Lumez application through Better Auth. Their names receive the __Secure- prefix in the HTTPS configuration. Authentication cookies use HttpOnly, which prevents direct access through browser JavaScript, and SameSite=Lax; these attributes do not replace the other security controls.

- better-auth.session_token: an identifier used to authenticate the session. Its configured persistent lifetime is 14 days. Active sessions may be renewed according to the authentication rules, so this is

not an absolute account retention period. A non-persistent sign-in uses a session cookie without that persistent expiry.

- better-auth.session_data: an encrypted cache of session and user information used to validate access with fewer database lookups. Its configured validity is 5 minutes; it may be refreshed while the session is used.

- better-auth.dont_remember: records the choice not to keep a persistent sign-in. It has no persistent Max-Age and follows the browser session. Browser session restoration settings can affect when session cookies are actually removed.

3. Two-factor authentication and trusted devices

These cookies are associated with the two-factor authentication flow when it is enabled for the account. Trusting a device is a choice in the sign-in flow; it does not authorize marketing or replace the account's security responsibilities.

- better-auth.two_factor: a temporary identifier linking the pending second-factor challenge to the sign-in flow, with a configured lifetime of 10 minutes.

- better-auth.trust_device: identifies a device that the user chose to trust for the second factor. Its configured lifetime is 30 days and can be renewed after a valid trusted-device sign-in. Removing it may cause the second factor to be requested again.

4. Language preference

The first-party lumez_locale cookie stores only the selected supported language code: en, es, pt or fr. It is written when the user saves a language choice, has a configured lifetime of 365 days, and may be replaced by a later choice. It is not an advertising identifier.

Without a saved preference, Lumez tries the browser's language preferences and then a country indication supplied in request headers by the infrastructure, if available. It falls back to English when no supported language can be determined. This flow does not request GPS access from the browser.

5. Local browser storage

Local storage is separate from cookies. The following records have no automatic time-based expiry in the reviewed code and can remain after the browser closes until an application action removes them or the user clears the site's storage. Signing out must not be understood as a guarantee that all local preferences have been erased.

- lumez:pending-onboarding: stores the company name and team-size range provided during registration so that setup can resume after email verification. The implemented flow removes it when onboarding is finished or when the stored record cannot be parsed. If the process is abandoned, there is no automatic expiry timer.

- lumez:grid:{workspace}:{user}:{screen}: where local table persistence is active, stores sorting, search text, filters, column choices, density and pagination. The key identifies the relevant workspace, user

and screen, or a local fallback. Search text or filters may contain personal information entered by the user. Records may be overwritten by later choices or removed when the view is reset; local deletion does not automatically delete a view saved on the server.

6. Third-party features and tracking

The reviewed application does not show an implemented advertising pixel or third-party behavioral analytics tracker. This finding concerns the reviewed code, not an independently verified production environment. It does not support a blanket claim that every deployment is free of third-party cookies or tracking.

If you open WhatsApp, Meta or another external service through a link, that service’s own storage practices and notices apply on its pages. A connection to a messaging channel does not by itself establish that its cookies are installed in the Lumez interface. Any later embedded feature must be assessed and included in this inventory before activation where required.

7. Necessity, choices and consent

Authentication and security storage is used to provide the signed-in service requested by the user. Language and view preferences support choices made while using the interface. Their legal treatment depends on their actual purpose and the applicable rules; calling a record functional does not automatically exempt it from every consent requirement.

Where prior consent is required, an optional technology must remain inactive until a valid choice is made, and refusal or withdrawal must be available without misleading controls. The reviewed version does not include a cookie banner or consent-management center. The need for those controls depends on the technologies actually deployed and the rules applicable in the markets served; a technology requiring consent must not be activated without the necessary controls.

8. Managing storage and requesting assistance

You can use your browser’s site-data controls to view, restrict or remove cookies and local storage for the Lumez domain. Clearing authentication cookies may sign you out or require another security check. Clearing language, onboarding or table records may remove those preferences or interrupt a setup in progress. Apply the controls on each browser or device you use.

Deleting browser storage does not delete the account, workspace, messages or server records. Data-subject requests follow the Privacy Policy and the Rights and Deletion document. Privacy and support requests may be sent to arthurgfcardozo@gmail.com or to Digital Directive at the postal address identified in these documents; authenticated export and deletion controls are available within their stated scope. Where processing relies on consent, withdrawal affects future consent-based processing and does not automatically undo processing that was lawful before withdrawal.